10/524854

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

IB 03/03374
20 AUG 2003

REC'D 03 SEP 2003
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 15 JUIL. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 G W / 010801

Réservé à l'INPI	
REMISE DES PIÈCES DATE 19 AOUT 2002 LIEU 99 N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0210463 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 19 AOUT 2002	1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE Patrice GUILLERM Schlumberger Systèmes Département Propriété Intellectuelle 50 avenue Jean-Jaurès, B.P. 620-12 92542 Montrouge cedex France
Vos références pour ce dossier *(facultatif)* 76.0708 FR - PG	

Confirmation d'un dépôt par télécopie	☒ N° attribué par l'INPI à la télécopie
2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé sécurisé d'échange de données entre un navigateur et un site WEB.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 DEMANDEUR (Cochez l'une des 2 cases)	☐ **Personne morale** ☐ **Personne physique**
Nom ou dénomination sociale	Schlumberger Systèmes
Prénoms	
Forme juridique	Société Anonyme
N° SIREN	5 6 2 1 1 3 5 3 0
Code APE-NAF	
Domicile ou siège — Rue	50 avenue Jean-Jaurès
Domicile ou siège — Code postal et ville	9 2 1 2 0 Montrouge
Domicile ou siège — Pays	France
Nationalité	Française
N° de téléphone *(facultatif)*	01 46 00 63 22 N° de télécopie *(facultatif)* 01 46 00 70 26
Adresse électronique *(facultatif)*	pguillerm@montrouge.sema.slb.com
	☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'[redacted]ITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES DATE 19 AOUT 2002
LIEU 99
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0210463

DB 540 G W / 010801

Vos références pour ce dossier : *(facultatif)*		76.0708 FR - PG
6 MANDATAIRE *(s'il y a lieu)*		
Nom		GUILLERM
Prénom		Patrice
Cabinet ou Société		Schlumberger Systèmes
N °de pouvoir permanent et/ou de lien contractuel		10219
Adresse	Rue	50 avenue Jean-Jaurès, B.P. 620-12
	Code postal et ville	9 2 5 4 2 Montrouge cedex
	Pays	France
N° de téléphone *(facultatif)*		01 46 00 48 65
N° de télécopie *(facultatif)*		01 46 00 70 26
Adresse électronique *(facultatif)*		pguillerm@montrouge.sema.slb.com
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'Inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Patrice GUILLERM
IP Engineer Cards

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Procédé sécurisé d'échange de données entre un navigateur et un site WEB.

Domaine technique

L'invention se rapporte à un procédé d'échange sécurisé de données entre deux dispositifs de traitement de données. La présente invention s'applique tout particulièrement à un échange de données entre un dispositif incluant de préférence une carte à puce dotée d'un navigateur (browser en anglais) et au moins une ressource informatique telle qu'un site WWW (World Wide Web) plus communément appelé site WEB (Web sites site en anglais), un serveur incluant des services, etc.

Le dispositif couplé à la carte à puce peut être d'un type quelconque. Ce système peut être de type embarqué ou non. Rappelons qu'un système embarqué est par exemple un téléphone mobile, un assistant électronique, un ordinateur portable, etc.

Le procédé de l'invention s'applique tout particulièrement aux communications utilisant un algorithme de chiffrement de type symétrique.

L'exemple qui servira à l'illustration de l'invention sera celui d'une carte à puce couplée à un système embarqué communicant avec une pluralité de ressources.

Etat de la technique

Une carte comprend généralement un navigateur (browser en anglais), également appelé logiciel de navigation par l'homme du métier. Ce navigateur donne la possibilité à un téléphone mobile d'accéder à des services en ligne ou à des services locaux de type WAP.

De manière à assurer un échange de données sécurisé entre un navigateur stocké dans la carte à puce et un site WEB, on emploi des moyens cryptographiques tels que le cryptage ou la signature électronique.

Il existe deux types de cryptographie :

- la cryptographie conventionnelle utilisant des clés symétriques,

- la cryptographie à clé publique utilisant des clés asymétriques.

L'utilisation de la cryptographie à clé publique requiert un espace mémoire important. Sa mise en œuvre présente d'énormes difficultés dans une carte à puce dans laquelle la taille mémoire est limitée en nombre d'octets. C'est pourquoi la plupart des navigateurs utilisent la cryptographie à clé symétrique. Cependant, l'utilisation de la cryptographie à clé symétrique pose aussi des problèmes dans une carte à puce. En effet, un navigateur ne peut pas stocker toutes les clés de tous les sites WEB avec lesquels il communique. Par conséquent, lorsque l'utilisateur du navigateur désire échanger des informations avec un site WEB de manière sécurisée, le site WEB doit initialement transmettre des clés au navigateur pour les utiliser ultérieurement lors d'opérations d'encryption et/ou de signature. Le problème aujourd'hui est que les sites WEB n'acceptent pas le partage de leurs clés avec d'autres sites WEB. En d'autres mots, si un site WEB "A" installe des clés dans un navigateur pour les utiliser ultérieurement, ce site WEB "A" refuse qu'un site WEB "B" puisse les effacer ou les utiliser.

Cette situation crée un "trou de sécurité" pour les transactions sécurisées basées sur l'encryption symétrique, et, par voie de fait, un manque de confiance à la fois de la part des utilisateurs et de la part des sites WEB.

L'invention

Un but de l'invention est d'obtenir une meilleure confiance en l'utilisation de la carte à puce pour réaliser des transactions.

L'invention concerne une carte à puce comprenant un navigateur pour communiquer avec un site WEB incluant des pages WEB, caractérisé en ce que

- le navigateur comprend une pluralité de zones privées, chaque zone privée pouvant être allouée à un ensemble de ressources respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée entre une zone privée et un ensemble de ressources ;

- et en ce qu' un programme assure qu'un ensemble de ressources communique exclusivement avec la zone privée qui lui est allouée.

Une zone privée comprend des données applicatives permettant d'établir une liaison sécurisée avec un ensemble de ressources. Ces données peuvent être des clés d'encryption symmétriques, des pages résidentes, etc.

A noter qu'un ensemble peut contenir un ou plusieurs sites WEB.

De cette façon, dans la carte, chaque zone peut être allouée à un ensemble de sites WEB particulier. Les données applicatives formant chaque zone privée ne sont donc accessibles que par l'ensemble de sites WEB concerné empêchant ainsi un autre ensemble de sites WEB d'utiliser une zone qui ne lui a pas été allouée.

L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple et faite en référence aux dessins annexés.

Dans les dessins :

La figure 1 est une vue d'un système informatique sur lequel peut s'appliquer l'invention.

La figure 2 est une vue schématique des différentes étapes illustrant un exemple d'échange de données entre un navigateur et une pluralité de sites WEB.

La figure 3 est une vue des deux grandes étapes constituant une transaction sécurisée.

Les figures 3 à 6 sont des vues schématiques des paramètres d'entrée et des paramètres de sortie d'exemples de programmes mettant en œuvre l'invention.

Description détaillée d'un exemple illustrant l'invention

Pour simplifier la description, les mêmes éléments portent les mêmes références.

La figure 1 représente un système informatique SYS. Dans notre exemple illustré, ce système inclus plusieurs navigateurs (BW1-BW2) stockés dans une carte à puce (CARD1-CARD2) respective. Dans notre exemple de réalisation, Chaque carte à puce (CARD1-CARD2) est couplée à un téléphone mobile respectif (MOB1-MOB2). A noter qu'un navigateur peut être stocké indifféremment dans la carte ou dans le téléphone mobile.

Un navigateur peut communiquer par l'intermédiaire d'un réseau RES avec une pluralité de sites WEB1 et WEB2. Généralement, un fournisseur d'accès AC s'intercale sur le réseau entre le navigateur (BW1-BW2) et un site WEB1-WEB2.

Dans notre exemple, chaque utilisateur UT1-UT2 interagit avec le navigateur BW1-BW2 respectif par l'intermédiaire d'une interface utilisateur respective GUI1 et GUI2.

Selon l'invention, chaque navigateur BW1 et BW2 comprend des zones privées ZP1-ZP2 et ZP3-ZP5, respectivement. Chaque zone privée comprend des données applicatives.

Pour des raisons de sécurité, ces différentes zones sont stockées dans la carte à puce. De cette façon, les zones ne sont accessibles que par le propriétaire de la carte à puce.

De préférence, chaque zone comprend :

- un paramètre VASid identifiant la zone privée en question. De préférence, cette valeur est une valeur fixée par défaut ;
- une clé VMK; Cette clé sera appelée clé maître dans la suite de la description ;
- éventuellement, une page d'accueil propre à la zone privée ;
- éventuellement, un ensemble de pages résidentes associées à la page d'accueil ;

De préférence, la valeur de la clé VMK est renseignée avant l'utilisation de la zone privée.

Dans notre exemple illustré, en référence à la figure 2, le procédé comprend deux étapes principales :

- A) l'authentification AUT,
- et B) l'administration ADM.

Dans notre exemple illustré, en référence aux figures 2 et 3, les étapes du procédé sont énumérées ci-dessous. A noter que dans l'exemple illustrant les étapes du procédé, on considère que l'utilisateur UT1 souhaite communiquer avec le site WEB1. Pour des raisons de simplification de l'exposé de l 'invention, la carte CARD1 et le téléphone mobile MOB1 n'ont pas été représentées sur la figure 3.

A) L'authentification

Etape 1

Initialement, l'utilisateur UT1 souhaite obtenir un service du site WEB1 et communiquer en toute sécurité avec ce site.

L'utilisateur contacte l'administrateur du site WEB1 et lui donne le nom du gestionnaire OP du navigateur BW1 ; La fonction de ce gestionnaire est notamment de fournir au site WEB1 certains paramètres qui lui permettront de communiquer avec la zone privée qui lui a été allouée et non une autre.

L'utilisateur peut également donner le nom du fournisseur d'accès AC à l'administrateur du site WEB1. Dans ce cas, dans l'étape 2, le site WEB1 contacte le gestionnaire OP par l'intermédiaire du fournisseur d'accès AC (ce cas est représenté par les lignes en pointillé sur la figure 3).

Etape 2

Lors d'une deuxième étape, le site WEB1 contacte le gestionnaire OP.

Etape 3

Ensuite, lors d'une troisième étape, le gestionnaire OP donne au site WEB1 toutes les informations pour procéder à un échange de données sécurisé avec une zone privée particulière. Dans notre exemple de réalisation, le gestionnaire fourni au site WEB1 :

- l'identifiant VASid ;
- la clé VMK ;
- et éventuellement d'autres informations telles que
  - la taille d'une page d'accueil et des pages résidentes dans la carte ;
  - le nombre de pages résidentes ;
  - l'identifiant du navigateur BWid.

Etape 4

Dans notre exemple de réalisation, l'administrateur du site WEB1 transmet, lors d'une quatrième étape, à l'utilisateur

- un identifiant USERID
- un mot de passe PW

De préférence, la transmission est réalisée par un moyen sécurisé tel qu'un courrier postal.

Dans notre exemple de réalisation, le site WEB1 stocke aussi ces deux paramètres dans une mémoire, ou une base de données BDD auquel il est connecté, pour une utilisation ultérieure.

Etape 5

Lors d'une cinquième étape, le site WEB1 transmet au navigateur BW1 une page incluant des champs à compléter. Dans notre exemple, ces champs correspondent :

- à l'identifiant USERID ;
- et au mot de passe PW.

Dans notre exemple, cette page inclus une référence propre à activer un programme VBA installé dans la carte.

Etape 6

Lors d'une sixième étape, le navigateur exécute le programme VBA. Le programme VBA a une fonction d'authentification et a pour but notamment
- de demander à l'utilisateur son identifiant USERID et son mot de passe PW
- et de construire une requête incluant par exemple l'identifiant USERID et le mot de passe PW.

Les différentes phases d'exécution de ce programme VBA sont énumérées ci-dessous.

Programme VBA :

Dans notre exemple de réalisation, et en référence à la figure 4, ce programme comprend des paramètres d'entrée PE1 et des paramètres de sortie PS1. Les paramètres d'entrée sont :
- la valeur de l'identifiant VASid de la zone privée allouée au site WEB1
- et des références à savoir :
  - l'identifiant USERID de l'utilisateur
  - le mot de passe PW de l'utilisateur.

Les paramètres de sortie PS sont :
- la valeur de l'identifiant VASid
- la valeur de l'identifiant USERID
- la valeur de l'identifiant du navigateur BW
- la valeur cryptée du mot de passe PW
- des données de sécurité telles qu'un nombre aléatoire, une signature, etc.

Ces paramètres de sortie sont stockés sous la forme d'une requête générée au cours de la phase 5 décrite ci-dessous.

Dans notre exemple de réalisation, l'exécution de ce programme comprend plusieurs phases :

Phase 1

Lors de la première phase, le programme VBA sélectionne la zone privée correspondant à l'identifiant VASid.

Phase 2

Le programme stocke, lors d'une deuxième phase, la valeur de l'identifiant USERID dans la zone privée.

Phase 3

Lors d'une troisième phase, le programme calcul une clé de session en utilisant la clé maître VMK connue à la fois du navigateur et du site WEB1, et d'autres paramètres tels que l'identifiant VASid, le nombre aléatoire, etc. Cette clé de session est calculée à partir d'un certain nombre d'informations: VMK, BWid, un nombre aléatoire, etc. Dans notre exemple de réalisation, cette clé a un rôle très temporaire. Elle ne sert qu'à crypter le mot de passe de l'utilisateur.

Phase 4

Lors d'une quatrième phase, le programme chiffre le mot de passe en utilisant la clé de session.

Phase 5

Lors d'une cinquième phase, le programme construit une requête.

Etape 7

Une septième étape consiste pour la carte à transmettre la requête au site WEB1.

Etape 8

Le site WEB1 vérifie la requête reçue, en l'occurrence l'identifiant USERID et le mot de passe PW. Pour ce faire, le site WEB1 génère d'abord la clé de session qui doit être identique à celle générée par le navigateur durant la phase

3 de l'étape 6. Le site WEB1 peut alors décrypter le mot de passe PW en utilisant la clé de session VMK ;Pour réaliser cette vérification, le site WEB1 interroge la base de données BDD, et compare l'identifiant et le mot de passe reçu du navigateur avec ceux préalablement stockés dans la base BDD.

Dans notre exemple, le site WEB1 calcule également la signature de la requête reçue à partir de la clé de session. Il compare ensuite le résultat avec la signature inclue dans le message.

Etape 9

Si le résultat de la vérification est positif, l'authentification est terminée. La zone privée et la carte peuvent communiquer. Dans notre exemple, Isi le résultat est positif, le site WEB1 transmet à la carte une page comprenant :

- un programme VA
- un programme IVK
- un programme IRP

Cette page, plus précisément les programmes associés, ont pour fonction d'administrer la zone privée allouée au site WEB1.

B) L'administration

L'authentification étant réalisée, l'administration de la carte est réalisée par l'intermédiaire de programmes (plug-in en anglais) qui permettent au navigateur d'utiliser la zone privée allouée à un site WEB1.

Par conséquent, lors de la neuvième étape, l'administration des zones privées débute. Le navigateur exécute cette page, à savoir l'ensemble des programmes. Les différentes phases d'exécution de l'ensemble des programmes VA, IVK, IRP sont énumérées dans la suite de la description.

Le programme VA

Premièrement, il exécute le programme VA. La figure 5 illustre un exemple schématique des entrées PE2 de ce programme. Le programme VA a une

fonction d'authentification. Ce programme autorise le site WEB1 d'être authentifié par le navigateur BW1.

Dans notre exemple, ce programme VA comprend des paramètres d'entrée PE2 et de sortie. Le paramètre de sortie est un signal informant si une transaction peut être lancée.. Les paramètres d'entrée PE2 sont dans notre exemple :

- la valeur de l'identifiant VASid qui permet au navigateur de sélectionner la zone privée adéquate ;
- la valeur de l'identifiant USERID ;
- des données de sécurité.

Exécution du programme VA

Dans notre exemple illustré, l'exécution de ce programme comprend plusieurs phases. Dans notre exemple, ces phases sont les suivantes :

Phase 1

Le programme sélectionne la zone privée correspondant à l'identifiant VASid.

Phase 2

Le programme vérifie la valeur de l'identifiant USERID avec celle stockée dans la zone privée.

Phase 3

Le programme calcul une clé de session VSK en utilisant la clé maître VMK ainsi que d'autres données, par exemple un nombre aléatoire, une signature, un compteur de synchronisation, etc.

Phase 4

Le programme VA vérifie les données de sécurité à savoir le nombre aléatoire, la signature, le compteur de synchronisation, etc. Cette vérification

permet de s'assurer que les données de sécurité associées à la zone privée en question correspondent aux données de sécurité de la zone privée allouée au site WEB1.

Si le résultat de la vérification est positif, le navigateur lance une transaction sécurisée avec le site WEB1 et la zone privée allouée. Dans la négative, aucune transaction n'est lancée et le navigateur affiche par exemple une page d'accueil publique.

De préférence, quand une transaction est lancée, la clé de session est stockée parce qu'elle peut être utilisée pendant toute une session. Cependant, dans notre exemple de réalisation, lorsque la transaction est terminée ou que le résultat de la vérification faite à la phase 4 est négatif, la clé de session est effacée.

Une transaction sécurisée reste ouverte pendant toute la durée de l'exécution de la page courante. De préférence, cette transaction est fermée quand le navigateur reçoit une nouvelle page. Par conséquent, si un site WEB désire utiliser une transaction sécurisée sur plusieurs pages, il devra insérer l'appel du programme VA au début de chacune des pages envoyées au navigateur.

Si une transaction est lancée, le navigateur peut exécuter les deux autres programmes IVK et IRP :

Le programme IVK

Ce programme a pour fonction le chargement de clés chiffrées dans la zone privée. Dans notre exemple de réalisation, ce programme comprend des paramètres d'entrée PE3 et un paramètre de sortie PS3. Dans notre exemple, les paramètres d'entrée sont des clés chiffrées qui peuvent être la clé maître VMK ou les clés de d'encryption/signature reçues du site WEB1. Ces clés

d'encryption/signature sont les clés symétriques citées dans le paragraphe "Etat de la technique". Elles font partie des "données applicatives" citées dans le paragraphe "l'invention". Ce sont elles qui seront utlisées ultérieurement pour encrypter ou signer des informations échangées entre le navigateur et le site WEB1.

Le paramètre de sortie est un signal informant que le chargement a été ou non réalisé avec succès.

Lorsque le navigateur exécute ce programme, il vérifie qu'une transaction est lancée. Si c'est le cas, le programme sélectionne la zone privée en question. Une fois la sélection effectuée, le programme décrypte les clés symétriques reçues du site WEB1 en utilisant la clé de session VSK et les stocke dans la zone privée. Le nombre de clés est quelconque.

Le programme IRP

Ce programme a pour fonction de charger soit une page d'accueil chiffrée dans la zone privée en question, soit une ou plusieurs pages résidentes chiffrées. Ces pages font partie des "données applicatives" citées dans le paragraphe "l'invention ".

Dans notre exemple de réalisation, ce programme IRP comprend un paramètre d'entrée CRP qui est une page résidente chiffrée issue du site WEB1. Cette page peut être soit une page d'accueil ou une page résidente. Le paramètre de sortie SCS/FAIL est un message indiquant si oui ou non l'installation des pages a été réalisée avec succès ou si au contraire l'installation a échoué.

Lorsque le navigateur exécute le programme IPR, il vérifie qu'une transaction sécurisée est lancée. Si c'est le cas, le programme sélectionne la zone privée en question. Ensuite, le programme décrypte la page reçue en utilisant la clé de session VSK et stocke la page dans la zone privée en question.

Etape 10

Lors de cette dixième étape, les différents résultats obtenus par les différents programmes lancés au cours de l'étape 9 sont transmis au site WEB1.

Etape 11

Lors d'une onzième étape, le site WEB1 vérifie les résultats obtenus par les différents programmes. Si les résultats obtenus conviennent, le site WEB1 peut utiliser sa zone privée. Dans notre exemple de réalisation, le site WEB1 peut réaliser des transactions utilisant les clés symétriques.

Etape 12

Lors d'une douzième étape, le site WEB1 transmet alors au navigateur une page qui comprend le programme VA, des opérations de signature ou de chiffrage, un lien vers une page résidente, etc.

Etape 13

Dans notre exemple, lorsque le navigateur a reçu cette page, la transaction est fermée. Le navigateur exécute alors le programme VA. Si le résultat de la vérification est positif, le navigateur lance une nouvelle transaction sécurisée avec le site WEB1 et la zone privée allouée. C'est la phase d'utilisation de la zone privée. Le site WEB1 peut ainsi réaliser des opérations de chiffrage et de signature en utilisant les clés symétriques associées à la zone privée en question. Le navigateur peut aussi accéder aux pages résidentes privées précédemment chargées par le programme IRP.

Cet exemple de réalisation montre bien qu'une ressource peut être indifféremment un site WEB, ou tout autre dispositif apte à communiquer avec une carte à puce.

On a vu notamment que l'autorisation d'utilisation d'une zone privée est réalisée par un programme comprend au moins un paramètre d'entrée correspondant à une clé d'accès à une zone. Dans notre exemple cette clé d'accès est constituée par le USERID et le mot de passe PW. On a vu aussi que la valeur de cette clé est fournie par l'ensemble des ressources concerné, c'est-à-dire l'ensemble des sites WEB dans notre exemple. Ce programme est apte après exécution et en fonction de cette clé à autoriser l'accès à une zone privée et interdire l'accès aux autres zones privées.

Dans notre exemple, on vu comment s'effectuait l'authentification entre une zone privée et le site WEB correspondant. L'ensemble de ressources transmet au navigateur une requête apte à demander à l'utilisateur d'entrer la clé d'accès reçue. Ensuite, si la clé d'accès est correcte, le dispositif comprend des instructions de code aptes à assurer la gestion de l'authentification entre un ensemble de sites WEB et la zone privée allouée correspondante.

On a vu aussi que le dispositif interprète des instructions de code aptes à assurer, après l'étape d'authentification et par l'intermédiaire des informations de sécurité, la gestion de l'administration des zones privées, ainsi que l'utilisation des données applicatives de ces zones privées pendant une communication entre le navigateur et le site WEB.

Dans notre exemple de réalisation, on a vu que les données de sécurité comprennent au moins une clé maître (VMK).

D'une manière générale, le procédé comprend les étapes suivantes :

- une étape de création d'une pluralité de zones privées, chaque zone privée pouvant être allouée à un ensemble de ressources respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée entre une zone privée et un ensemble de ressources ;
- une étape d'allocation d'une zone privée à un ensemble de ressources,

- une étape de communication entre ladite zone privée allouée et l'ensemble des ressources concerné, un programme interdisant tout accès à une autre zone privée pendant cette communication.

Avantageusement, on a vu que l'allocation d'une zone privée est gérée par une entité centralisée OP. Cette entité alloue une zone privée de la carte à l'ensemble des ressources WEB en lui fournissant des informations comprenant au moins:
- la référence (VASId) de la zone privée,
- et la valeur d'une clé maître (VMK) stockée au préalable dans la zone privée correspondante.

Dans notre exemple, on a vu que l'ensemble de ressources (WEB) transmet par un moyen de transmission sécurisé au moins une clé d'accès associée à une zone privée, ladite clé étant utilisé pour l'exécution d'un programme apte, après exécution, à autoriser l'accès à une zone privée et interdire l'accès aux autres zones privées.

Dans notre exemple, on a vu aussi que, afin d'ouvrir une transaction sécurisée, l'ensemble de ressources (WEB1) transmet un programme apte à vérifier si les informations de sécurité inscrites dans la zone privée (ZP1) correspondent aux informations de sécurité stockées dans une mémoire rattachée à l'ensemble de ressources (WEB1).

On a vu dans notre exemple de réalisation que la mise en œuvre de ce procédé nécessite l'installation d'un programme dans le dispositif. Ce programme d'ordinateur comprend au moins un paramètre d'entrée correspondant à une clé d'accès à une zone, la valeur de cette clé étant fournie par l'ensemble des ressources concerné, ledit programme étant apte après exécution en fonction de cette clé à autoriser l'accès à une zone privée et interdire l'accès aux autres zones privées.

Avantages

Grâce à ce mécanisme de "cloisement" des informations accessibles par un navigateur, les clés d'encryption et les pages locales associés à une zone privée n'est accessible que par le site WEB concerné et non par d'autres sites WEB.

Par conséquent, ce mécanisme de cloisonnement permet l'accès uniquement au site WEB qui les a installées.

La présente solution répond aussi à un second besoin du marché concernant l'installation de pages locales (dites "résidentes") accessibles par le navigateur. Les sites WEB peuvent installer des pages locales de façon sécurisée, et en permettre l'accès à l'utilisateur qu'après authentification de celui-ci. Ces pages locales étant "la propriété" d'un site WEB particulier, elles ne peuvent plus être effacées par l'installation de pages provenant d'un autre site WEB.

Revendications

1. Dispositif de traitement de données (MOB1) apte à communiquer avec une pluralité de ressources (WEB1,WEB2)par l'intermédiaire d'un navigateur (BW1), caractérisé en ce que:
- le navigateur (BW1) comprend une pluralité de zones privées (ZP1-ZP2), chaque zone privée pouvant être allouée à un ensemble de ressources (WEB1) respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée entre une zone privée (ZP1) et l'ensemble de ressources (WEB1) ;
- et en ce qu'il comprend un programme apte à assurer qu'un ensemble de ressources (WEB1)communique exclusivement avec la zone privée (ZP1) qui lui est allouée.

2. Dispositif selon la revendication 1, caractérisé en ce que ledit programme comprend au moins un paramètre d'entrée (USERID,PW) correspondant à une clé d'accès à une zone, la valeur de cette clé d'accès étant fournie de façon sécurisée par l'ensemble des ressources concerné (WEB1), ledit programme étant apte après exécution et en fonction de cette clé à autoriser l'accès à une zone privée (ZP1), et interdire l'accès aux autres zones privées (ZP2) du navigateur (BW1).

3. Dispositif selon la revendication 1 ou 2, caractérisé en ce que pour l'authentification, l'ensemble de ressources (WEB1) transmet au navigateur une requête apte à demander à l'utilisateur d'entrer la clé d'accès (USERID,PW) reçue, et en ce que si la clé d'accès est correcte, le dispositif comprend des instructions de code aptes à assurer la gestion de l'authentification entre un ensemble de ressources (WEB1) et la zone privée allouée (ZP1) correspondante.

4. Dispositif selon la revendication 1 ou 3, caractérisée en ce qu'il interprète des instructions de code aptes à assurer, après l'étape d'authentification et par l'intermédiaire des informations de sécurité, la gestion de l'administration des zones privées, ainsi que l'utilisation des données applicatives de ces zones privées pendant une communication entre le navigateur et le site WEB.

5. Dispositif selon la revendication 1, caractérisé en ce que les informations de sécurité comprennent au moins une clé maître (VMK).

6. Dispositif de traitement de données (MOB1) couplé à une carte à puce (CARD1) apte à communiquer avec une pluralité de sites (WEB1) par l'intermédiaire d'un navigateur (BW1), caractérisé en ce que:
- e navigateur comprend une pluralité de zones privées (ZP1-ZP2), chaque zone privée pouvant être allouée à un ensemble de sites respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée avec un ensemble de sites;
- et en ce que, le navigateur (BW1) interprète des instructions de code aptes à assurer qu'un ensemble de sites (WEB1) communique exclusivement avec la zone privée (ZP1) qui lui est allouée.

7. Procédé de communication entre un dispositif de traitement de données (MOB1) comprenant un navigateur (BW1) et un ensemble de ressources (WEB1), caractérisé en ce qu'il comprend les étapes suivantes :
- une étape de création d'une pluralité de zones privées (ZP1-ZP2), chaque zone privée pouvant être allouée à un ensemble de ressources respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée entre une zone privée et un ensemble de ressources ;
- une étape d'allocation d'une zone privée (ZP1) à un ensemble de ressources (WEB1),

- une étape de communication entre ladite zone privée allouée (ZP1) et l'ensemble des ressources (WEB1) concerné, un programme interdisant tout accès à une autre zone privée pendant cette communication.

8. Procédé selon la revendication 7, caractérisé en ce que l'allocation d'une zone privée (ZP1) est gérée par une entité centralisée (OP), et en ce que cette entité alloue une zone privée (ZP1) de la carte (CARD1) à l'ensemble de ressources (WEB1) en lui fournissant des informations comprenant au moins:
- la référence (VASId) de la zone privée ZP1,
- et la valeur d'une clé maître (VMK) stockée au préalable dans la zone privée (ZP1) correspondante.

9. Procédé selon la revendication 7, caractérisé en ce que l'ensemble de ressources (WEB1) transmet par un moyen de transmission sécurisé au moins une clé d'accès (USERID, PW) associée à une zone privée (ZP1), ladite clé étant utilisée pour l'exécution d'un programme apte, après exécution, à autoriser l'accès à la zone privée (ZP1) et interdire l'accès aux autres zones privées (ZP2).

10. Procédé selon la revendication 7, caractérisé en ce que, afin d'ouvrir une transaction sécurisée, l'ensemble de ressources (WEB1) transmet un programme apte à vérifier si les informations de sécurité inscrites dans la zone privée (ZP1) correspondent aux informations de sécurité stockées dans une mémoire rattachée à l'ensemble de ressources (WEB1).

11. Programme d'ordinateur pour un dispositif de traitement de données apte à communiquer avec une pluralité de ressources par l'intermédiaire d'un navigateur, caractérisé en ce que le navigateur comprend une pluralité de zones privées, chaque zone privée pouvant être allouée à un ensemble de ressources respectif et pouvant stocker des informations de sécurité propre à assurer une communication sécurisée entre une zone privée et un ensemble de ressources ; et en ce que le programme comprend au moins un paramètre d'entrée

correspondant à une clé d'accès à une zone, la valeur de cette clé étant fournie par l'ensemble des ressources concerné, ledit programme étant apte après exécution en fonction de cette clé à autoriser l'accès à une zone privée et interdire l'accès aux autres zones privées.

5

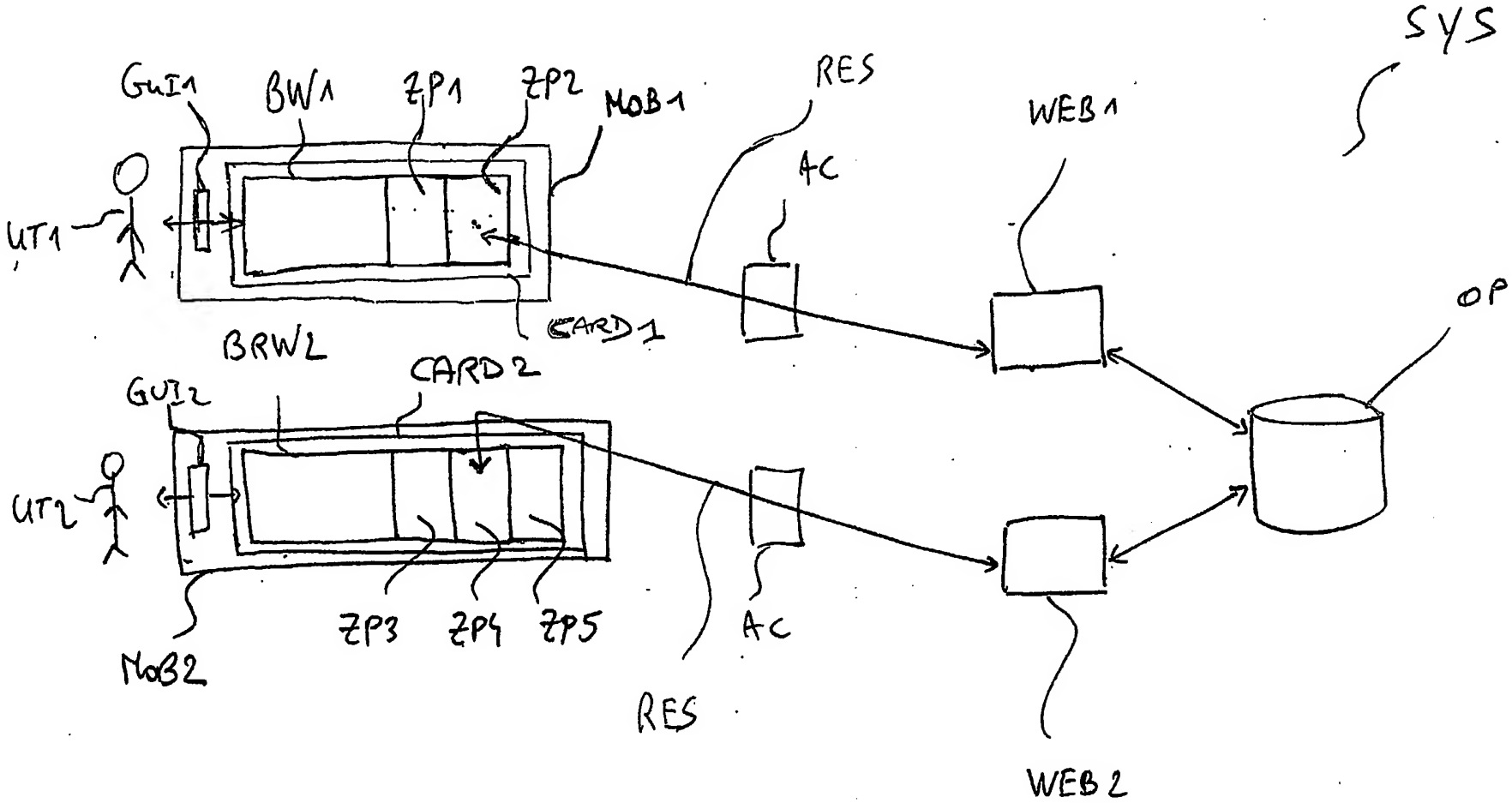

SYS
GUI1
BW1
ZP1
ZP2
MOB1
RES
AC
WEB1
UT1
BRW1
CARD1
OP
GUI2
CARD2
UT2
ZP3
ZP4
ZP5
AC
MOB2
RES
WEB2

figure 1

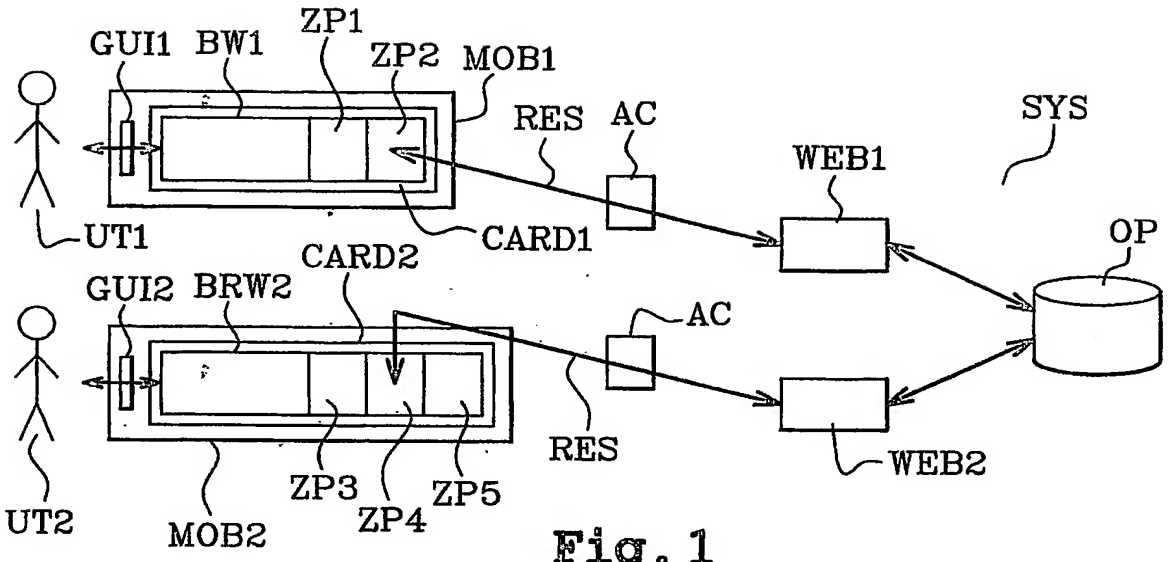

GUI1
BW1
ZP1
ZP2
MOB1
RES
AC
SYS
WEB1
UT1
CARD1
OP
CARD2
GUI2
BRW2
AC
RES
WEB2
ZP3
ZP4
ZP5
UT2
MOB2

Fig. 1

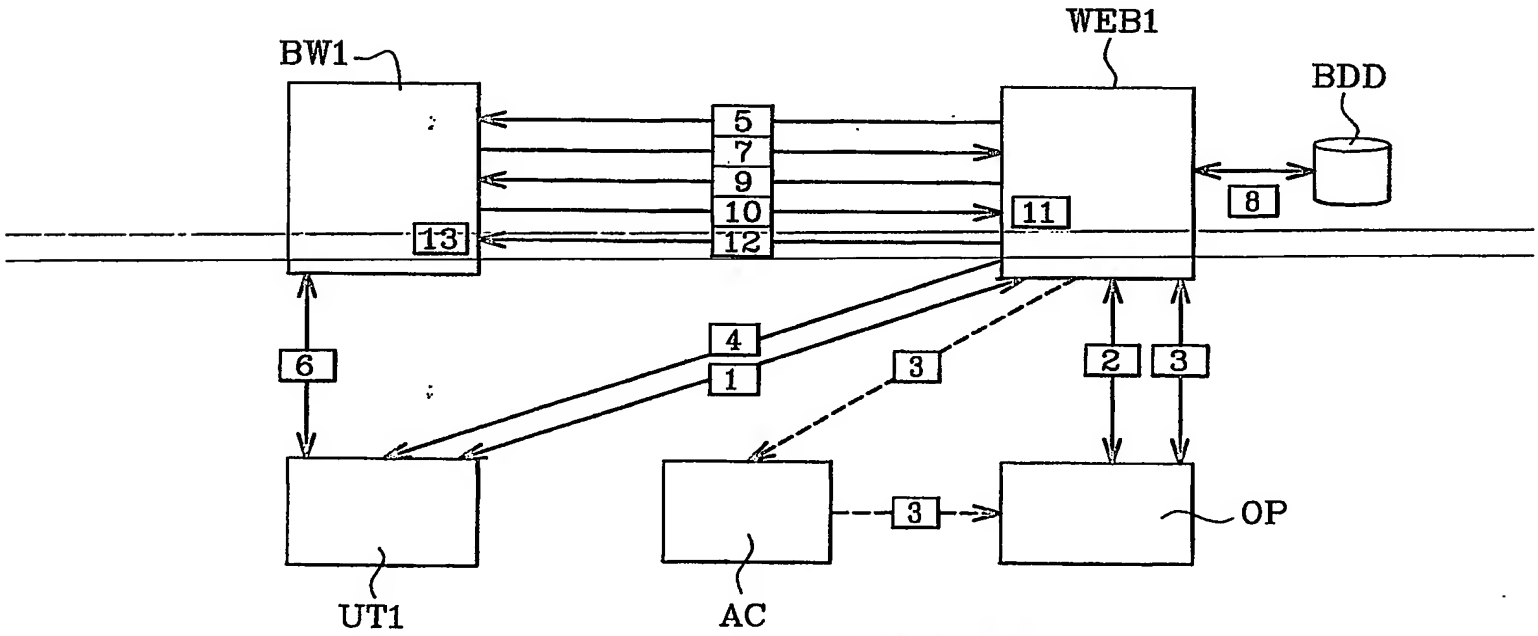

BW1
WEB1
BDD
5
7
9
10
12
13
11
8
6
4
1
3
2
3
3
OP
UT1
AC

Fig. 3

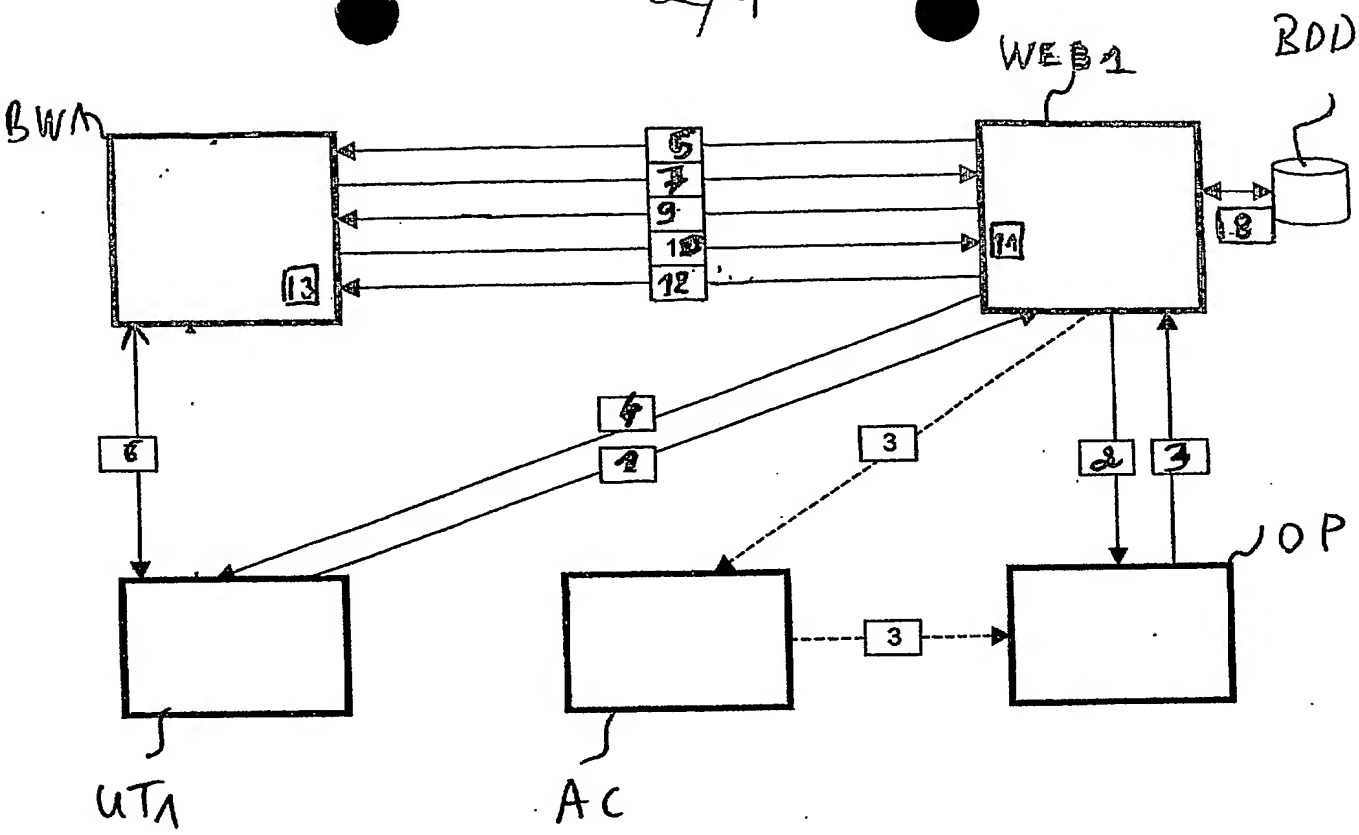


Figure 3

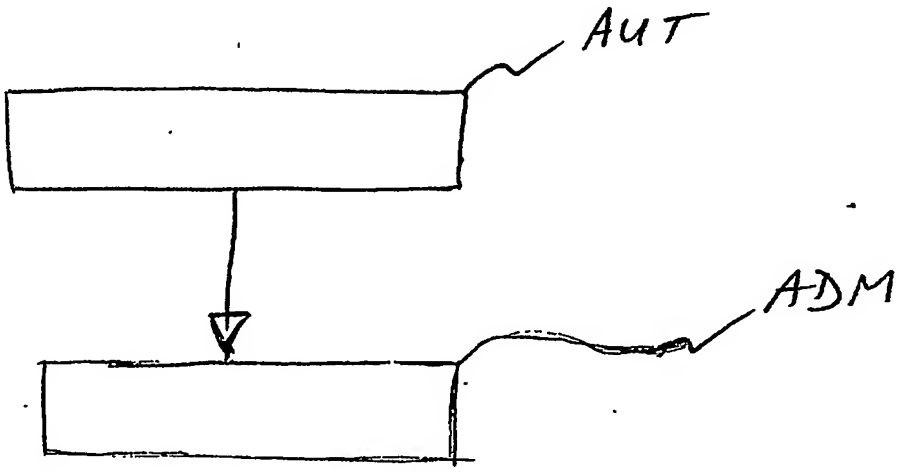


Figure 2

Fig. 2

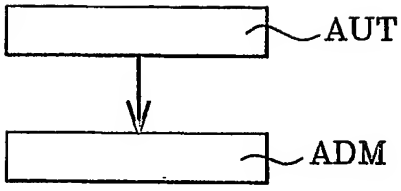


Fig. 4

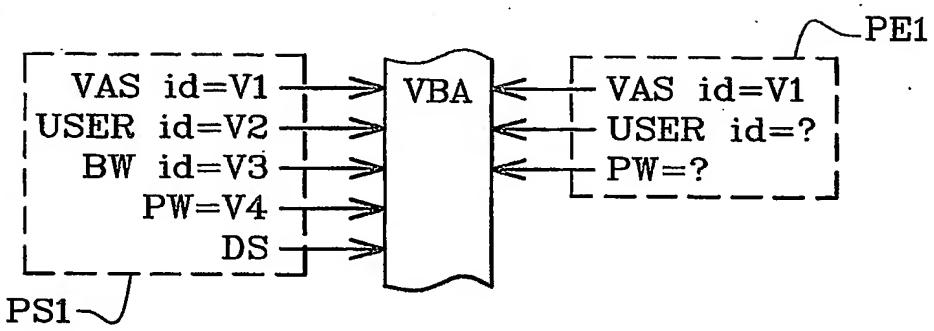


Fig. 5

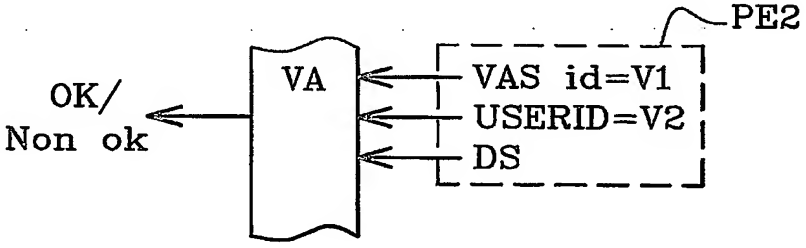


Fig. 6

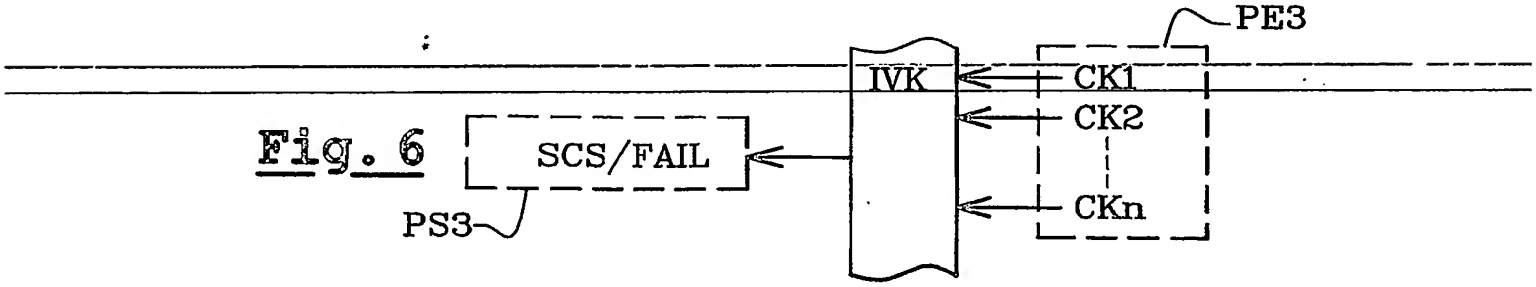
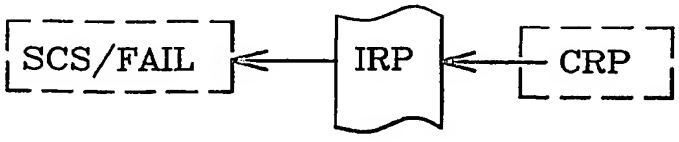


Fig. 7



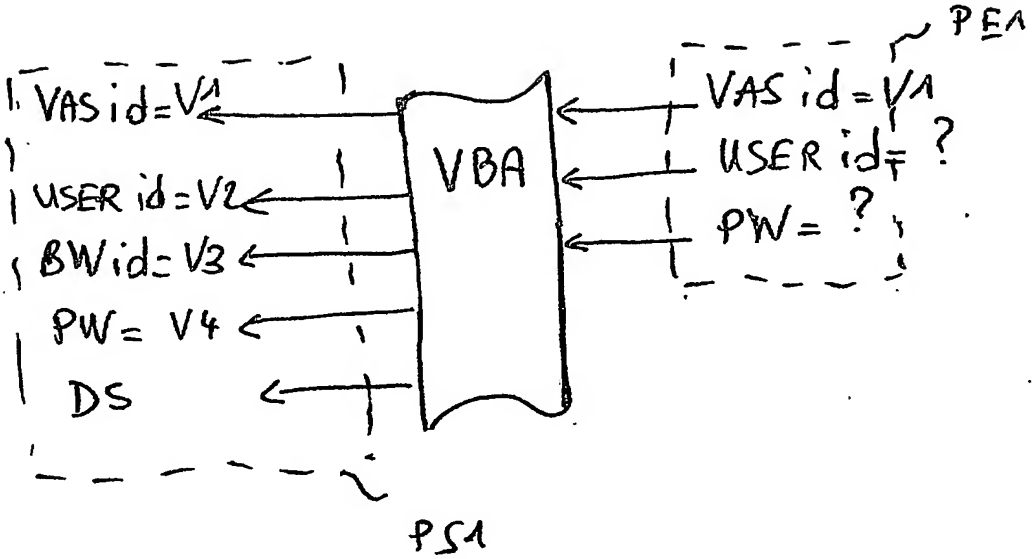


figure 4

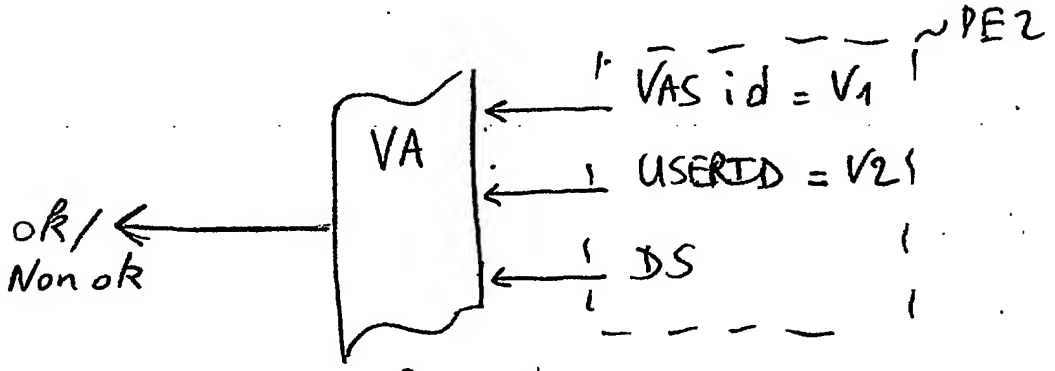


figure 5

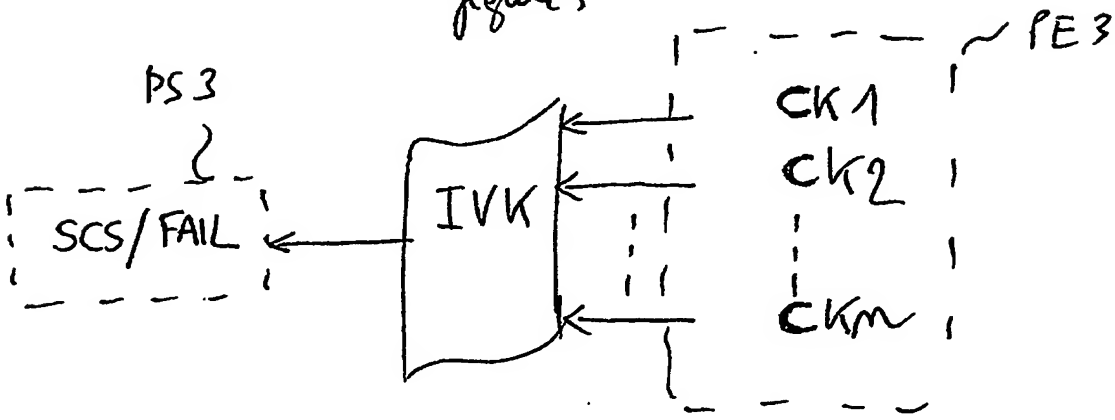


figure 6

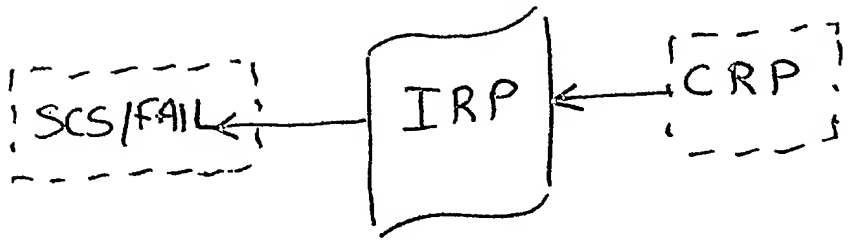


figure 7.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

Certa

N° 11 235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	76.0708 FR - PG
N° D'ENREGISTREMENT NATIONAL	0210463

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé sécurisé d'échange de données entre un navigateur et un site WEB.

LE(S) DEMANDEUR(S) :

Schlumberger Systèmes
50 avenue Jean-Jaurès
92120 Montrouge
France

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		SENDRA
Prénoms		François
Adresse	Rue	9 square Saint-Charles
	Code postal et ville	75012 Paris
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Patrice GUILLERM
IP Engineer Cards

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.